Wearable Smart Devices: Innovations Through AI and Cyberbiosecurity Threats

Ashley Purnell[1,3], Michaela Barnett[4], Lucas Potter[1-3] and Xavier Lewis-Palmer[1-4]
[1]School of Cybersecurity, Old Dominion University, Norfolk, VA, USA
[2]BIOSView Labs, Oswego, KS, USA
[3]Cyberlinc, Franklin, VA, USA
[4]Black in Cybersecurity, Washington, DC, USA

apurn003@odu.edu
michaela@bichq.org
lpott005@odu.edu
biosview@protonmail.com

Abstract: The integration of commercial health wearables (CHWs) with artificial intelligence (AI) has created innovative smart devices that provide continuous monitoring, analysis, and insights to improve health-related outcomes. They also help users to improve their physical fitness and detect early warning signs of health-related irregularities. Available over-the-counter, certain smartwatches and fitness trackers also aid in combating chronic and debilitating conditions like cardiovascular disease (CVD), which is the leading global cause of death (Brunier et al, 2020; Shajari et al, 2023). Exacerbated by the comorbid prevalence of obesity and diabetes, the treatment and management of CVD in the U.S. amounts to over $840 billion annually (Brunier et al, 2020). AI-powered CHWs are tools that help individuals make better daily health-related decisions to improve their cardiovascular health and fitness through automated analysis of critical biomarkers (e.g. blood pressure, heart rate, sleep patterns, and physical activity) and generative health-specific text alerts and recommendations. The advancements in cloud-based computing, data storage, nanotechnology in computer engineering, and integration of machine learning algorithms enable the data obtained from CHWs biometric sensors to be analyzed at rapid speeds. The acceptance of CHWs is increasing in popularity. In 2022, North American consumers purchased 42% of smart fitness trackers sold globally amounting to over $52 billion in sales. This commercial biotechnology industry is projected to have an annual growth rate of 17.6% (Laricchia, 2024). While CHWs are empowered by AI-enabled precision healthcare features, they also elevate the risk of cyberbiosecurity (CBS) threats (Jordan et al, 2020; Pauwels, 2023). CHWs, a repository of network-connected personal biological datasets, are vulnerable to unauthorized access, data corruption, inaccurate health recommendations, denial of user access, and potential risks to health and physical well-being outcomes (Affia et al, 2023). Cybercriminals use networked devices to execute destabilizing and malicious attacks on industries, governments, nations, and individuals causing financial, resource, reputational, and physical harm. However, CBS is an emerging field that studies the security risks that arise from the convergence of biotechnology systems enabled with internet access (DiEuliis et al, 2018; Guise et al, 2024). To protect against and mitigate CBS threats, consumers and developers of AI-powered CHWs must remain aware of the evolving CBS threats and employ methods to protect against unauthorized cyber breaches.

Keywords: Artificial intelligence, Cyberbiosecurity, Cardiovascular disease, Wearable smart devices

1. Introduction

The public pursuit of physical fitness exploded onto the market in the 1980s with the rise of athletic clubs and continues to maintain prominence in the U.S. fitness industry, representing over $30 billion in revenue annually (Gough, 2023). However, over 50% of new gym members with sedentary lifestyle habits drop out within six months (Linke et al, 2012). The Center for Disease Control has published numerous reports on or in relation to the importance of physical activity and healthy eating habits to lower the risks of cardiovascular disease, diabetes, metabolic syndrome, certain cancers, bone and muscle loss, and infectious diseases (Richards et al, 2014; Carande-Kulis, 2022). To improve health related outcomes, the Physical Activity Guidelines for Americans recommend that adults engage in a minimum of 2.5 hours of moderately intensive physical activity and 2 days of muscle strengthening activities weekly. Yet, over 46% of U.S. adults fail to meet either of these minimum standards (Elgaddal, 2022). Some major barriers to physical fitness include lack of time, support, financial resources, motivation, and knowledge about proper exercise techniques. While personal trainers, weight loss programs, health logs, and basic fitness trackers exist on the market, none have shown significant improvements in sustained engagement for inactive adults (Rippe, 2018).

Cardiovascular disease (CVD) is a chronic illness, and its risks can be reduced by more than 80% through improving daily lifestyle habits such as nutrition, exercise, weight management, sleep patterns, smoking cessation, and reducing chronic stress (Rippe, 2018). However, CVD remains one of the most debilitating medical conditions and the leading cause of death in adults globally (Brunier et al, 2020). CVD is a group of illnesses that affect the heart and blood vessels, including conditions such as pulmonary embolisms, cardiac arrhythmias, coronary artery disease, congestive heart failure, and stroke (i.e. cerebrovascular accidents and hemorrhagic brain aneurysms). The comorbid prevalence of obesity and diabetes exacerbates the outcomes of these conditions. In the U.S. the total cost of medical treatment and management of CVD is over $840 billion annually (Brunier et al, 2020). Individuals chronically affected by this condition often experience physical and functional impairments, difficulty maintaining employment, and a reduced life expectancy. These challenges can have a cascading effect on overall quality of life leading to psychological distress, financial hardship, strained relationships, and social disconnection (Lui et al, 2023).

Commercial health wearables (CHWs), specifically smartwatches and fitness trackers, became popular in the 2010s by companies such as Apple, Fitbit, and Garmin. Throughout the late 2010s and early 2020s, major CHW developers focused on advancing the accuracy of their biosensors and integrating artificial intelligence (AI) algorithms with predictive analytic capabilities (Kaur, 2024). While additional longitudinal studies are needed, preliminary research suggests that individuals who use AI-powered CHWs demonstrate a statistically significant increase in physical activity and healthy lifestyle habits over a 6-month period (Ferguson et al, 2022). In addition, athletic clubs and fitness trainers have reported a 25% increase in member retention and engagement rates when AI-enabled exercise equipment and software applications (apps) are incorporated into workout regimens (Vigue, 2024). CHWs hold significant promise as a tool to improve long-term healthy lifestyle choices, which can help to lower risks of CVD. However, as smart devices that store large amounts of personal biometric data, CHWs also present significant risks to the cybersecurity and cyberbiosecurity threat landscapes.

2. Methods

This paper reviewed literature on published research, industry reports, and conference proceedings related to commercial health wearables. The scope included peer-reviewed academic articles, grey literature, and technical specifications of devices such as the Apple Watch and Oura Ring, covering the years 2012 to 2024. The literature was selected based on relevance to commercial health wearable devices, cybersecurity risks, health monitoring effectiveness, and broader implications in cyberbiosecurity and healthcare systems. Databases such as IEEE, PubMed, Frontiers, and Springer were searched using key terms including "cyberbiosecurity," "wearable health devices," "IoT security," "healthcare cybersecurity," "fitness trackers," and "wearable biometric monitoring". Relevant industry sources, including Statista, Apple, Oura Health, FDA documentation, WHO publications, and reports from cybersecurity ventures, provided supplemental insights on market trends, device specifications, cybersecurity incidents, and regulatory implications. Studies addressing the effectiveness of wearable devices in detecting health conditions (Apple, 2020; Dusheck, 2017; Grzesiak et al, 2021), cybersecurity vulnerabilities specific to health wearables (Affia et al, 2023; Griffy-Brown et al, 2022; Silva-Trujillo et al, 2023), and broader cyberbiosecurity contexts (Chatzis et al., 2024; Elgabry et al, 2024; Reed et al, 2019) were critically analyzed. Meta-analysis studies such as those conducted by Ferguson et al (2022) were leveraged to evaluate the effectiveness

of commercial wearables in promoting health behaviors. Limitations towards the method have reduced the scope of review, and a follow-up article with an expanded scope is pending.

3. Revolution of Commercial Health Wearables Through Artificial Intelligence

CHWs have made significant progress in personal fitness technology over the past decade, enabling users to monitor their physical health through real-time biometric data analysis. Early CHW models, such as the Apple Watch released in 2015, introduced continuous biometric data monitoring and alerted users to irregular measurements or low activity (Chandel et al, 2022). While these devices were innovative for their time, they required further biotechnological research and design improvements to address data accuracy and increase computational power for more extensive data analytic capabilities. Over the next five years, major CHW companies invested in developing improved sensor designs (Lui et al, 2022). For example, Apple Watch redesigned their electrocardiogram (ECG) app, proprietary photoplethysmography biosensor (PPG) and cardiac biosensors to enhance the effectiveness and accuracy of their single-lead ECG detection systems (Isakadze et al, 2020). The 12-lead ECG is a federally regulated medical device that detects atrial fibrillation (AFib), a serious heart rhythm condition that, if left untreated, can lead to health complications such as blood clots, CVD, sudden cardiac arrest, cognitive decline, and dementia (National Library of Medicine, 2024). CHWs are considered wellness tools and are not federally regulated to meet quality standards for effectiveness and safety (Scheid et al, 2023). However, in 2018 and 2020, the Apple Watch Series 4 and the Fitbit Sense, respectively, were approved as Class II medical devices by the U.S. Food and Drug Administration (FDA) due to their ECG app accuracy being equivalent to the 12-lead ECG in detecting AFib incidents (Apple, 2020; Shih, 2022). Similar advancements in other biosensors have improved the speed, accuracy, detection, and analysis of various physiological changes (refer to Table 1). These ongoing innovations in CHWs help individuals address various health-related issues such as sleep quality, daily stress levels, fall risk detection, and tracking menstrual cycles and ovulation windows for family planning.

Table 1: Commercial Health Wearable Sensors

Sensor	Data Measurements
Accelerometer	Step count, distance, speed, caloric expenditure, fall detection, sleep quantity, sleep apnea
Electrocardiogram Sensor (ECG)	Electrical heart pulse rate to detect heart arrhythmias
Global Position System (GPS)	Geographic location, distance, speed, elevation
Gyroscope	Changes in angular rotation and directional speed that improves motion tracking, fall detection, and step count accuracy
Photoplethysmography (PPG)	Heart rate, irregular heart rhythms, respiratory rate, and blood oxygen saturation (SpO_2)
Negative Temperature Coefficient (NTC) Thermistor	Skin temperature and in conjunction with PPG provides physical exertion, stress estimation, menstrual cycle prediction, and ovulation tracking
Electrodermal Activity (EDA)	Sweat gland activity and with NTC and PPG sensors provides stress arousal levels

Biosensors have experienced exponential growth in capacity and capabilities due to advancements in computer engineering, nanotechnology, and the integration of AI. These innovations enable the activation of autonomous and complex AI computations for biometric data analysis (refer to Table 2), providing personalized insights and feedback that are easily accessible for consumers (Shajari et al, 2023). For example, DL algorithms are used in the Apple Watch ECG app, which is responsible for the improved speed (analysis within 30 seconds) and accuracy in AFib detection (Apple, 2020). RNN, CNN, and Gen AI algorithms are integrated into the Oura Labs section of the Oura Ring app providing metabolic analysis and insights to improve nutritional choices (Shajari et al, 2023). These AI algorithms are also utilized for early detection and monitoring of illnesses such as upper respiratory infections (e.g. common cold, influenza, and the coronavirus) with 80%-96% accuracy (Grzesiak et al, 2021; Shajari et al, 2023; Oura Team, 2024). Large language models and natural language processing algorithms are also utilized in the Oura Ring's Oura Advisor feature. Essentially, a health assistant chatbot, Oura Advisor uses the analytical results of an individual's biometric data to generate personalized health and fitness recommendations (Lemire, 2024). Additionally, most CHWs are compatible with third-party apps integrated with AI that monitor various health and fitness biometrics.

Table 2: Artificial Intelligence Contribution to Commercial Health Wearables

Category	Description
Machine Learning (ML)	Broad subfield of artificial intelligence that trains a computer to autonomously analyze and identify patterns, correlations, and insights from large datasets
Deep Learning (DL)	Subfield of ML that uses artificial neural networks that can analyze multiple large datasets and identify patterns and insights extracted from complex analysis
Convolutional Neural Networks (CNNs)	DL algorithm that specializes in analyzing movement data in a grid format using pattern recognition analysis to classify different forms of physical activity
Generative Artificial Intelligence (Gen AI)	DL algorithm trained on large datasets of text and data to provide pattern recognition and autonomously generates text, recommendations, and insights
Large Language Model (LLM)	Subfield of natural language processing that uses DL algorithms trained on large datasets of text to learn complex language patterns and rules to understand and generate coherent, relevant, human language text
Recurrent Neural Networks (RNNs)	DL algorithm that actively analyzes present and historical datasets to improve accuracy of pattern recognition and improved long term personalized insights

As AI networks autonomously analyze larger amounts of data over extended periods of time, they become more accurate in developing personalized baselines and identifying outlier data points that can assist in critical early detection and prevention recommendations. Through long term use, CHWs become rich repositories of personalized health data stored within apps and cloud servers. Every year, more consumers are flocking to these devices with over 42% of the market share of CHW fitness trackers being sold in North America. In 2023, global annual sales were over $52 billion with a projected annual growth rate of 17.6% (Laricchia, 2024). The ongoing exploration of AI's computational capabilities in CHWs and third-party apps will lead to exponential opportunities to improve monitoring, early detection, prevention, and the development of precision healthcare tools for acute, chronic, and rare diseases (Dusheck, 2017).

4. Fourth Industrial Revolution and Public Healthcare Innovations

CHWs and third-party health and fitness apps represent a unique sector of the bioeconomy. They contain sensitive health information, yet they are not federally regulated or classified as medical devices. CHWs are classified as Internet of Things (IoT) devices, exemplifying how innovations in historical fitness and wellness trackers are merging with the biotechnology sector amid the Fourth Industrial Revolution (4IR) (Silva-Trujillo et al, 2023). Characterized by enhanced efficiency, productivity, convenience, and task automation, the 4IR is digitally transforming and connecting aspects of our physical, biological, and digital lives that were historically separate (Park, 2016; Shankar et al, 2023). CHWs are now equipped with components and computational power that can significantly reduce lifestyle risk factors that contribute to chronically debilitating and lethal conditions like CVD and AFib. Alongside the advancements of CHWs, the field of biotechnology is also experiencing unprecedented growth in diagnosing, treating, and preventing diseases that exacerbate conditions such as CVD.

The 4IR has extended to traditional medical devices, referred to as the Internet of Medical Things (IoMT) devices such as implantable cardiac defibrillators, glucose monitors, insulin pumps, and neural implants serve crucial roles in the healthcare industry (Lesaja, et al, 2020; Griffy-Brown et al, 2022; Cinar et al, 2023). They are especially important as society faces challenges of a global increase in the aging population alongside chronic diseases, shortages of healthcare professionals, remote access to disease monitoring and treatment, and bridging gaps in care during global public health crises (Affia et al, 2023; Kohler et al, 2024; Mathkor et al, 2024). The COVID-19 pandemic in 2020 significantly accelerated the digital transformation of healthcare and life sciences (Chatzis et al, 2023). For instance, biosafety laboratories focused on pathogenic research, surveillance, diagnosis, and biopharmaceuticals evolved into smart labs, or Laboratories of the Future (LoTF) (Reed et al, 2019; Cinar et al, 2023; Crawford et al, 2023). These LoTF designs integrated laboratory automation, mobile robotic chemists, and advanced research tools like CRISPR-Cas9 to expedite research on SARS-CoV-2 (coronavirus). By combining functional genomic research and gene-editing tools with AI computations, scientists were able to better understand the genetic functions of the coronavirus and rapidly identify antiviral opportunities (Tomulescu, 2021; Deol et al, 2022). In 2024, innovations in the biotechnology industry contributed over $1.64 trillion to the global economy, with projections to exceed $5.84 trillion annually by 2034 (Polaris Market Research, 2024).

5. Cyberbiosecurity Threats in the Public Health Sector

However, advances in the healthcare landscape coexists with the constant threat to its cybersecurity. As the 4IR progresses with its revolutionary digital innovations, the cybercriminal industry runs parallel, utilizing the same technological advances to breach these cyber spaces (Elgabry et al, 2024). In 2021, the global cost and damage from cybercrimes were estimated to be $6 trillion, and it is projected to surpass $10.5 trillion by the end of 2025 making cybercrime the third most profitable economy behind the U.S. and China (Morgan, 2020). Shankar et al (2023) noted that between 2020 and 2023, over 93% of healthcare organizations experienced a cybersecurity breach. Exploiting cyber-based vulnerabilities, cybercriminals target companies and individuals for various motives, including corporate espionage, theft of product research and design intellectual property, malicious attacks to sabotage corporate reputation, data exfiltration to develop precision marketing and advertising, identity and insurance fraud, extortion, and ransom attacks (McGuire, 2018; Jordan et al, 2020; Lacher, 2023; Barsky, 2024). Studies show that CHWs, IoT devices, and IoMT devices are common targets of cyber-attacks, such as malware injection, spoofing, distributed denial of service, man-in-the-middle, eavesdropping, and botnet attacks (Griffy-Brown et al, 2022; Silva-Trujillo et al, 2023; Barnett et al, 2024). Silva-Trujillo et al (2023) conducted an analysis of Bluetooth pairing vulnerabilities on seven smart watches and found that minimum security requirements were not met to prevent Bluetooth-level cyber breaches, creating an entry point for hackers to intercept, exfiltrate, and maliciously alter data. Furthermore, as AI continues to revolutionize the capabilities of these devices, their associated apps, and compatible third-party apps, they will become increasingly desirable targets for unauthorized access and exploitation.

The risks to CHWs and the biotechnology industry extend beyond economic concerns. They pose the risk of not only financial and competitive losses but also potential loss of life, and impact military and geopolitical operations. For instance, the FDA recalled cardiac defibrillators manufactured by Abbott and insulin pump models made by Medtronic due to cybersecurity vulnerabilities (Kuehn, 2018; Klonoff et al, 2019). These vulnerabilities allowed for the manipulation of configuration settings, premature draining of device batteries rendering them inoperable, and triggering the devices to randomly administer potentially lethal cardiac shocks and insulin overdoses. In June 2023 during the ongoing Russian-Ukrainian War, a former Russian submarine commander connected to a deadly 2022 missile attack in Ukraine was tracked by a Ukrainian citizen through his

Strava app's GPS data and murdered in suspected retaliation (Wright, 2023). Also in that same year, U.S. military members received suspicious GEEKINFIT 18 smartwatches that powered on automatically and connected to Wi-Fi and Bluetooth-enabled devices, raising concerns about a potential malware attack to access sensitive personnel and military base data (Bonenberger, 2023).

Each cyber-enabled device and its associated software introduces unique cybersecurity vulnerabilities and risks to the overall digital infrastructure, making cyberspace a perfectly ambiguous grey zone that can be exploited for political and ideological influences, as well as cyberwarfare operations and real-world bioterrorism threats (Dixon, 2021). Cybercrime has evolved, with some groups capable of executing advanced persistent threats (APTs) using sophisticated and often undetectable methods of system intrusion, data exfiltration, opportunities for malicious encoding, and network footholds for future cyber-attacks (Palmer et al, 2022). The advances in digital computational technology converge with critical biotechnological progress, creating a significant blind spot where cybercriminals thrive. The extent to which cybercrime combined with the application of biological components as an attack chain, that can escalate into acts of war, seems to be a recent exploration (Palmer et al, 2021a). However, the degree to which biological misinformation can spread and enable further acts of aggression has not yet been fully considered (Palmer et al, 2021b). A more diverse author pool may help in better defining threat horizons in emerging biocrime forms and their countermeasures, as the current pool of thought by existing authors is deemed insufficient (Elgabry et al, 2024).

It is in part due to these intersecting cyber risks in the biotechnology field that Murch et al (2018) proposed the need for a new field of study known as cyberbiosecurity (CBS). CBS involves "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of commingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience" (Murch et al, 2018). These data breaches also pose a growing threat to national and global security due to the increasing digital presence of bioagent research and design data and the growing accessibility to generate weaponized bioagents and threats of biowarfare (George, 2019; Lentzos, 2020; Potter et al, 2021;). For example, breaches in biopharmaceutical and genomic research labs can lead to data corruption resulting in the creation and release of precision maladies, hypervirulent pathogens, sabotage of drug manufacturing formulations, misdiagnosis, inaccurate or lack of access to patient treatment, and interruption of biological and healthcare supply chains (Guttieres et al, 2019; Cebo, 2022; Berche, 2023; Crawford et al, 2023; Gostin et al, 2023; Chatzis et al, 2024).

6. Policy, Regulatory, and Consumer Recommendations

Realistically, achieving a zero-threat cyber environment is not possible. The value of cybercrime is exponentially growing as the 4IR continues to rapidly digitize and automate societies and individuals' daily lives and operations. However, what is possible is decreasing the probability of an attack and mitigating the impact of a breach with preparedness plans (Shankar et al, 2023). Currently, the U.S. regulatory system is a fragmented legacy framework (e.g. CFAA, DFAR, FD&C Act, FTC Act, HIPAA, ITADA) that lags behind the revolutionary innovations and growth that CHWs and the bioeconomy are experiencing (McNicholas et al, 2024). CHWs are becoming abundant sources of predictive biometric datasets, making the need for applicable regulatory standards even more significant in terms of implementing policy, audits and best practice standards. In 2022, the FDA approved the Institute of Electrical and Electronics Engineers (IEEE) Standards Association's IEEE 2621 Medical Device Cybersecurity Certification Program to address the growing cybersecurity risks of IoMT medical devices. IEEE 2621 establishes an internationally recognized industry standard for medical devices ensuring they meet national cybersecurity best practices such as risk management assessments and mitigation, privacy by design, and secure software lifecycle development (Olabi-Colón and Ruth, 2024). It is essential to bring together multidisciplinary specialists representing the intersections of CBS threats, international leaders in the biotechnology industry, and policymakers to address the growing cyber vulnerabilities posed by the convergence of CHWs, IoT devices, and IoMT devices.

Griffy-Brown et al (2022) recommended that manufacturers utilize a life cycle approach similar to the IEEE 2621 certification, which assesses risks to consumers, processes, technology, and protects devices throughout conception, development, operation, and disposal stages. Implementing a cybersecurity framework (e.g. NIST, ISO 27001/27002, HITRUST, and CIS Critical Security Controls) that provides best practice standards for identifying, monitoring, and mitigating security risks, while also staying informed about evolving adversarial tactics, techniques and procedures (TTPs) employed by threat actors through resources like MITRE ATT&CK, are essential references to address cybersecurity risks (Tomulescu, 2021). Additionally, an agile governance approach that emphasizes international collaboration and flexible responses to evolving threats can potentially minimize inequality in societies and companies excluded from these conversations while also remaining abreast of global TTPs (Pauwels, 2023). Utilizing AI's computational capacity to develop more robust strategies for intrusion detection, protocol monitoring, encryption and authentication solutions, emergency mitigation response plans, and recovery strategies (Guttieres et al, 2019).

Consumers can better safeguard their data by increasing their awareness of CBS and IoT threats to determine which devices they truly need to be network-enabled. This can help reduce the number of devices that could potentially be at risk of a cyber breach. Once consumers have identified their essential devices, they should carefully choose products from reputable companies with a track record of protecting consumer data and providing firmware updates, rather than opting for devices from lesser-known, bargain-priced companies. To enhance security, it is important to enable all available device security features, limit data collection by devices and apps to the minimum necessary, change default passwords, enable multi-factor authentication, sign up for manufacturer notifications of recalls and security alerts, and avoid using jailbroken technology from unofficial sources. Lastly, consumers should track their devices' end-of-life cycle to promptly remove them from the home network and replace them as needed. Implementing network segmentation within a personal home network can also help reduce the risk of sensitive data being breached by other IoT devices.

7. Limitations

This study encountered several limitations. The rapidly evolving nature of commercial wearable technology and cybersecurity threats presents inherent challenges to comprehensive coverage. Some sources relied upon were industry-focused, which might introduce biases favoring positive reporting of device capabilities and understated risks. Moreover, the cybersecurity risks associated with health wearables are often underreported or selectively reported, making it difficult to achieve an exhaustive assessment. Publications by Barsky (2024) and Klonoff et al (2019) highlighted significant cyber incidents but also indicated limitations in the availability of comprehensive incident data due to proprietary restrictions or privacy concerns. Additionally, variability in the methodology and scope of the analyzed studies (Ferguson et al., 2022; Griffy-Brown et al., 2022; Silva-Trujillo et al., 2023) may affect the generalizability and comparability of findings. Studies using device-specific metrics or proprietary software, such as those by Apple (2020) and Oura Team (2024), limited the replicability and independent verification of results. Future research should include more independent, large-scale studies with standardized cybersecurity assessment frameworks (Olabi-Colón & Ruth, 2024) and emphasize comprehensive reporting of cyber incidents to ensure better comparability and generalizability.

8. Conclusion

The convergence of CHWs, AI-powered algorithms, automation and biotechnological innovations will continue to improve over-the-counter consumer access to advanced computational health and fitness tools. This offers the potential to track positive health trends, record bioinformatic information, and mitigate health risk factors that affect quality of life. CHWs are becoming a vital part of the biotechnology industry. A balanced perspective must be presented alongside indications of further technological integration in CHWs and similar devices. While CHW devices are beneficial for monitoring and managing health, they face significant security challenges that we are still navigating. It is imperative to develop a more robust custom framework in which issues are reviewed and considered against relevant emerging threats. Addressing these vulnerabilities with stronger security standards and robust data protection measures is essential to ensure user safety and maintain trust in wearable health technology. Recognizing that numerous societal factors will increase humans' dependence on external devices for health monitoring, Affia et al (2023) recommend "defending forward" at the intersection of AI innovations, quantum computing, and the evolutions of the 4IR's impact on technologies. CHW manufacturers and all potential consumers must pay shared attention to the risks posed by medical or lifestyle advances that accompany the innovations of automation and digitization that characterize this 4IR.

References

Affia, A. *et al.* (2023) "IoT Health Devices: Exploring Security Risks in the Connected Landscape", *Internet of Things*, Vol. 4, No. 2, pp 150-182. https://doi.org/10.3390/iot4020009

Apple. (2020) "Using Apple Watch for arrhythmia detection", Apple, https://www.apple.com/healthcare/docs/site/Apple_Watch_Arrhythmia_Detection.pdf

Barnett, M. *et al.* (2024) "Botnet in Healthcare: Threats, Vulnerabilities, and Mitigation Strategies", In Proceedings of the 23rd European Conference on Cyber Warfare and Security, Vol. 23, No. 1, pp 58-65.

Barsky, N. (2024) “UnitedHealth Paid Hackers $22 million, Fixes Will Soon Cost Billions”, Forbes, https://www.forbes.com/sites/noahbarsky/2024/04/30/unitedhealths-16-billion-tally-grossly-understates-cyberattack-cost/

Berche, P. (2023) “Gain-of-Function and Origin of Covid 19”, *La Presse Medicale*, Vol. 52, No. 1. https://doi.org/10.1016/j.lpm.2023.104167

Bonenberger, A. (2023) “Warning Issued to Troops Receiving Strange Smart watches in the Mail”, Military News, https://www.military.com/daily-news/2023/06/22/warning-issued-troops-receiving-strange-smartwatches-mail.html

Brunier, A. and Muchnik, A. (2020) “WHO Reveals Leading Causes of Death and Disability Worldwide: 2000-2019”, World Health Organization, https://www.who.int/news/item/09-12-2020-who-reveals-leading-causes-of-death-and-disability-worldwide-2000-2019

Carande-Kulis, V., Elder, R.W. and Matson-Koffman, D. (2022) “Standards Required for the Development of CDC Evidence-Based Guidelines”, *MMWR Supplements*, Vol. 71, No. 1, pp 1-6.

Cebo, D. (2022) “Strategical Analysis of Cyberbiosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Threats”, *TechRxiv*. https://doi.org/10.36227/techrxiv.20485929.v1

Chandel, R.S. *et al.* (2022) “Smart Watches: A Review of Evolution in Bio-Medical Sector”, *Materials Today: Proceedings*, Vol. 50, No. 5, pp 1053-1066. https://doi.org/10.1016/j.matpr.2021.07.460

Chatzis, I. *et al.* (2024) “Cyberbiosecurity: A Threat of the Sages”, In Biosecurity in the Making: The Threats, the Aspects and the Challenge of Readiness, pp 119-132, CRC Press, Boca Raton.

Cinar, B. and Thomas, R.K. (2023) “Cyber-biosecurity: A Paradigm Shift in the Field of Life Sciences and Agriculture Sector” *Asian Journal of Biotechnology and Genetic Engineering,* Vol. 6, No. 1, pp 58-75.

Crawford, E. *et al.* (2023) “Cyberbiosecurity in High-Containment Laboratories”, *Frontiers in Bioengineering and Biotechnology*, Vol. 11, July. https://doi.org/10.3389/fbioe.2023.1240281

Deol, P. *et al.* (2022) “CRISPR use in diagnosis and therapy for COVID-19”, *Journal of Microbiological Methods*, Vol. 50, pp 123-150. https://doi.org/10.1016/bs.mim.2022.03.002

DiEuliis, D., Lutes, C.D. and Giordano, J. (2018) “Biodata Risks and Synethetic Biology: A Critical Juncture”, *Journal of Bioterrorism and Biodefense*, Vol. 9, No. 1. https://doi.org/10.4172/2157-2526.1000159

Dixon, T. (2021) “The Grey Zone of Cyber-Biological Security”, *Internal Affairs*, Vol 97, No. 3, pp 685-702. https://doi.org/10.1093/ia/iiab041

Dusheck, J. (2017) “What your wearable knows; Changes in usual patterns can tip you off to illness”, Stanford Medicine, https://stanmed.stanford.edu/what-wearable-biosensors-including-a-smart-watch-can-tell-you-about-your-health/

Elgabry, M. and Johnson, S. (2024) “Cyber-biological Convergence: A Systematic Review and Future Outlook” *Frontiers in Bioengineering and Biotechnology*, Vol. 12, September, https://doi.org/10.3389/fbioe.2024.1456354

Elgaddal, N., Kramarow, E. and Reuben, C. (2022) “Physical Activity Among Adults Aged 18 and Over: United States, 2020. National Center for Health Statistics Data Brief”, Center for Disease Control, https://www.cdc.gov/nchs/products/databriefs/db443.htm#:~:text=Summary-,In%202020%2C%2024.2%25%20of%20adults%20aged%2018%20and%20over%20met,Hispanic%20origin%2C%20and%20family%20income.

Ferguson, T. *et al.* (2022) “Effectiveness of Wearable Activity Trackers to Increase Physical Activity and Improve Health: A systematic Review and Meta-Analyses” *Lancet Digital Health*, Vol. 4, No. 9, pp 615-626. https://doi:10.1016/S2589-7500(22)00111-X

George, A.M. (2019) “The National Security Implications of Cyberbiosecurity”, *Frontiers in Bioengineering and Biotechnology*, Vol. 7, March. https://doi.org/10.3389/fbioe.2019.00051

Gostin, L.O. and Gronvall, G.K. (2023) “The Origins of Covid-19 – Why It Matters (and Why It Doesn’t)”, *New England Journal of Medicine*, Vol. 388, No. 25. https://doi: 10.1056/NEJMp2305081

Gough, C. (2023) “Gym, Health & Fitness Club Industry Revenue in the United States 2010-2023”, Statista, https://www.statista.com/statistics/605223/us-fitness-health-club-market-size-2007-2021/#:~:text=Gym%2C%20health%20%26%20fitness%20club%20industry,the%20United%20States%202010%2D2023&text=The%20revenue%20of%20the%20fitness,billion%20U.S.%20dollars%20in%202023

Griffy-Brown, C. *et al.* (2022) “Cyber Risk Case Analysis in Wearable and Medical Devices: Developing a Cyberbio Security Risk Framework”. In 2022 Portland International Conference on Management of Engineering and Technology, pp 1-6. https://doi.org/10.23919/PICMET53225.2022.9882739

Grzesiak, E. *et al.* (2021) “Assessment of the Feasibility of Using Noninvasive Wearable Biometric Monitoring Sensors to Detect Influenza and the Common Cold Before Symptom Onset” *Journal of the American Medical Association Network Open,* Vol 4, No. 9. https://doi.org/10.1001/jamanetworkopen.2021.28534

Guise, N. *et al.* (2024) “2023 Cyberbiosecurity Summit Underscores Challenges Associated with Cybersecurity and the Rapidly Growing Bioeconomy”, *Global Security: Health, Science and Policy*, Vol. 9, No. 1. https://doi.org/10.1080/23779497.2024.2401164

Guttieres, D. *et al.* (2019) “Cyberbiosecurity in Advanced Manufacturing Models”, *Frontiers in Bioengineering and Biotechnology*, Vol. 7, September. https://doi.org/10.3389/fbioe.2019.00210

Isakadze, N. and Martin, S.S. (2020) “How Useful is the Smartwatch ECG?”, *Trends in Cardiovascular Medicine*, Vol. 30, No. 7, pp 442-448. https://doi.org/10.1016/j.tcm.2019.10.010

Jordan, S., Fenn, S. and Shannon, B. (2020) “Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity”, *IEEE*, Vol. 53, No. 10, pp 59-68, https://doi: 10.1109/MC.2020.2995578

Kaur, J. (2024) *Technological Enhancements for Improving Employee Performance, Safety, and Well-Being*, IGI Global, Hershey.
Klonoff, D. and Han, J. (2019) "The First Recall of a Diabetes Device Because of Cybersecurity Risks", *Journal of Diabetes Science and Technology,* Vol. 13, No. 5, pp 817-820. https://doi.org/10.1177/1932296819865655
Kohler, C. *et al.* (2024) "The Value of Smartwatches in the Health Care Sector for Monitoring, Nudging, and Predicting: Viewpoint on 25 Years of Research", *Journal of Medical Internet Research*, Vol. 26. https://doi.org/10.2196/58936
Kuehn, B. (2018) "Pacemaker Recall Highlights Security Concerns for Implantable Devices", *Circulation American Heart Association Journal*, Vol. 138, No. 15, pp 1597-1598. https://doi.org/10.1161/CIRCULATIONAHA.118.037331
Lacher, T. (2023) "Why Medical Records are 10 Times More Valuable Than Credit Card Info?", LinkedIn, https://www.linkedin.com/pulse/why-medical-records-10-times-more-valuable-than-card-lacher-cissp/
Laricchia, F. (2024) "Apple Watch Unit Sales Worldwide 2015-2023", Statista, https://www.statista.com/statistics/1421546/apple-watch-sales-worldwide/
Lemire, J. (2024) "Smart Ring Maker Oura Launches Generative AI-powered Assistance Called Oura Advisor", Sports Business Journal, https://www.sportsbusinessjournal.com/Articles/2024/07/09/oura-advisor
Lentzos, F. (2020) "How to Protect the World from Ultra-Targeted Biological Weapons", *Bulletin of the Atomic Scientists*, Vol. 76, No. 6, pp 302-308.
Lesaja, S. and Palmer, X.L. (2020) "Barin-Computer Interfaces and the Dangers of Neurocapitalism", *arXiv*. https://doi.org/10.48550/arXiv.2009.07951
Linke, S., Gallo, L. and Norman, G. (2012) "Attrition and Adherence Rates of Sustained vs. Intermittent Exercise Interventions", *Annals of Behavioral Medicine*, Vol. 42, No. 2, pp 197-209. https://doi: 10.1007/s12160-011-9279-8
Lui, G.Y. *et al.* (2022) "The Apple Watch for Monitoring Mental Health-Related Physiological Symptoms: Literature Review", *Journal of Medical Internet Research Mental Health*, Vol. 9, No. 9. https://doi.org/10.2196/37354
Lui, J. *et al.* (2023) "Impact of New Cardiovascular Events on Quality of Life and Hospital Costs in People With Cardiovascular Disease in the United Kingdom and United States", *Journal of the American Heart Association*, Vol. 12, No. 19. https://doi: 10.1161/JAHA.123.030766
Mathkor, D. *et al.* (2024) "Multirole of the Internet of Medical Things (IoMT) in Biomedical Systems for Managing Smart Healthcare Aystems: An Overview of Current and Future Innovative Trends", *Journal of Infection and Public Health,* Vol 17, No. 4, pp 559-572. https://doi.org/10.1016/j.jiph.2024.01.013
McGuire, M. (2018) *Into The Web of Profit: Understanding the Growth of the Cybercrime Economy*, Bromium Inc, Cupertino.
McNicholas, E.R. and Faircloth, F.E. (2024) *Cybersecurity Laws and Regulations: USA 2025*, ICLG, London.
Morgan, S. (2020) "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
Murch, R. *et al*. (2018) "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy". *Frontiers in Bioengineering and Biotechnology*, Vol 6, April. https://doi: 10.3389/fbioe.2018.00039
National Library of Medicine. (2024) "Atrial fibrillation", Medline Plus. https://medlineplus.gov/atrialfibrillation.html
Olabi-Colón, T. and Ruth, C. (2024). "First Test Facilities and Products Recognized Under New IEEE Cybersecurity Certification Program for Medical Devices", IEEE Standards Association. https://standards.ieee.org/news/ieee-2621-first-certification-recognition/
Oura Team. (2024) "What's new in Oura Labs?", Oura Health. https://ouraring.com/blog/oura-labs/?srsltid=AfmBOoqN9L2kbW84CCG1OCYToJ8lRKUDdDWbxtp0S7K15tflPf87RaYi
Palmer, X., Powell, E. and Potter, L., (2021a, June) "Biocyberwarfare and Crime: A Juncture of Rethought", In Proceedings 20th European Conference on Cyber Warfare and Security, Vol. 22, No. 1, pp 517-524, Academic Conferences International Limited, Reading.
Palmer, X.,Powell, E. and Potter, L. (2021b) "Matters of Biocybersecurity With Consideration to Propaganda Outlets and Biological Agents", In Proceedings 20th European Conference on Cyber Warfare and Security, Vol. 22, No. 1, pp 525-534, Academic Conferences International Limited, Reading.
Palmer, X., Potter, L. and Karahan, S. (2022) "An Exploration on APTs in Biocybersecurity and Cyberbiosecurity", In Proceedings 17th International Conference on Cyber Warfare and Security, Vol. 17, No. 1, pp 532-535. https://doi.org/10.34190/iccws.17.1.67
Park, H. (2016) "Are We Ready for the Fourth Industrial Revolution?", *Yearbook of the Medical Informatics*, Vol. 10, No. 1, pp 1-3. https://doi: 10.15265/IY-2016-052
Pauwels, E. (2023) "How to Protect Biotechnology and Biosecurity from Adversarial AI Attacks? A Global Governance Perspective", In Cyberbiosecurity: A New Field to Deal with Emerging Threats, pp 173-184, Springer, Princeton.
Polaris Market Research. (2024) "Biotechnology Market Size, Share, Trends, Industry Analysis Report: By Technology Application", Polaris Market Research. https://www.polarismarketresearch.com/industry-analysis/biotechnology-market
Potter, L., Ayala, O. and Palmer, X. (2021) "Biocybersecurity: A Converging Threat as an Auxiliary to War", In Proceedings 16th International Conference on Cyber Warfare and Security, pp 291-298, Academic Conferences International Limited, Reading.
Reed, J.C. and Dunaway, N. (2019) "Cyberbiosecurity Implications for the Laboratory of the Future", *Frontiers in Bioengineering and Biotechnology*, Vol 7, August. https://doi.org/10.3389/fbioe.2019.00182

Richards, C.L., Iademarco, M.F. and Anderson, T.C. (2014) "A New Strategy for Public Health Surveillance at CDC: Improving National Surveillance Activities and Outcomes", *Public Health Reports*, Vol. 129, No. 6, pp 472-476. https://doi.org/10.1177/003335491412900603

Rippe, J. (2018) "Lifestyle Strategies for Risk Factor Reduction, Prevention, and Treatment of Cardiovascular Disease", *American Journal of Lifestyle Medicine*, Vol. 13(2), pp 204-212. doi:10.1177/1559827618812395

Scheid, J.L., Reed, J.L. and West, S.L. (2023) "Commentary: Is Wearable Fitness Technology a Medically Approved Device? Yes and No", *International Journal of Environmental Research and Public Health*, Vol. 20, No. 13. https://doi.org/10.3390/ijerph20136230

Shajari, S. *et al*. (2023) "The Emergence of AI-Based Wearable Sensors for Digital Health Technology: A Review", *Sensors*, Vol. 23, No. 23. https://doi.org/10.3390/s23239498

Shankar, D.D. *et al.* (2023) "Data Mining for Cyber Biosecurity Risk Management – A Comprehensive Review", *Computers & Security*, Vol 137, February. https://doi.org/10.1016/j.cose.2023.103627

Shih, J. (2022) "Fitbit Irregular Rhythm Notifications: Indications for Use", U.S. Food and Drug Administration, https://www.accessdata.fda.gov/cdrh_docs/pdf21/K212372.pdf

Silva-Trujillo, A.G. *et al.* (2023) "Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack", *Sensors*, Vol. 23 No. 12. doi.org/10.3390/s23125438

Tomulescu, C. (2021) "Cyberbiosecurity. A short review", In Proceedings Smart Cities International Conference (SCIC) Vol. 9, pp 9-26, National Institute for Chemical-Pharmaceutical R&D, Bucharest.

Vigue, A. (2024) "Gym Member Retention Strategies for 2025", Trainerize. https://www.trainerize.com/blog/gym-member-retention-strategies/

Wright, G. (2023) "Ukraine War: Russian Ex-Navy Commander Shot Dead While Jogging in Krasnodar", BBC. https://www.bbc.com/news/world-europe-66162502